

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**APPEAL BRIEF UNDER 37 C.F.R. § 41.37**

Mail Stop: Appeal Brief-Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief under 37 C.F.R. § 41.37 is submitted in support of the Notice of Appeal filed February 28, 2008, responding to the Final Office Action mailed November 28, 2007.

It is not believed that extensions of time or fees are required to consider this Appeal Brief. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. §1.136(a), and any fees required therefor are hereby authorized to be charged to Deposit Account No. 08-2025.

### **I. Real Party in Interest**

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

### **II. Related Appeals and Interferences**

There are no known related appeals or interferences that will affect or be affected by a decision in this Appeal.

### **III. Status of Claims**

Claims 1-2 and 4-21 stand finally rejected. Claim 3 has been canceled. No claims have been allowed. The final rejections of claims 1-2 and 4-21 are appealed.

### **IV. Status of Amendments**

No amendments have been made subsequent to the final Office Action mailed November 28, 2007. The claims in the attached Claims Appendix reflect the present state of Applicants' claims.

## **V. Summary of Claimed Subject Matter**

The claimed inventions are summarized below with reference numerals and references to the written description ("specification") and drawings. The subject matter described in the following appears in the original disclosure at least where indicated, and may further appear in other places within the original disclosure.

Embodiments according to independent claim 1 describe a method of detecting a non-virus component in a virus-protected computer system having antivirus software. The method comprises identifying a software trace of the non-virus component, Applicants' specification, page 4, lines 13-15, and conveying the trace to the computer system as a virus pseudo-signature to allow detection of the non-virus component by the system's antivirus software. Applicants' specification, page 4, lines 18-21. The component is a hardware device and the software trace is indicative of the presence of the hardware device in the computer system. Applicants' specification, page 5, lines 7-14.

Embodiments according to independent 11 describe a method of facilitating the detection of a non-virus component in a first virus-protected computer system. The method comprises identifying, on a second computer system, a software trace of the non-virus component and conveying the trace towards an antivirus update source. Applicants' specification, page 4, lines 13-21. The software trace may be passed, as a virus pseudo-signature, to the first computer system. Applicants' specification, page 5, lines 3-14. The component is a hardware device and the software trace is indicative of the presence of the hardware device in the first computer system. Applicants' specification, page 5, lines 7-14.

Embodiments according to independent claim 12 describe a method of detecting, in a virus-protected computer system, the presence of a non-virus component. The method comprises receiving a virus pseudo-signature associated with a software trace of the non-virus component, Applicants' specification, page 5, lines 3-14, and comparing the pseudo-signature with software traces disposed within the system's memory. Applicants' specification, page 3, lines 1-2. The component is a hardware device and the software trace is indicative of the presence of the hardware device in the computer system. Applicants' specification, page 5, lines 7-14.

Embodiments according to independent claim 14 describe an apparatus for detecting, in a virus-protected computer system, a non-virus component. The apparatus comprises a pseudo-signature generation element operative to produce a software trace of the non-virus component, Applicants' specification, page 3, lines 1-5 and page 5, lines 6-12, and an antivirus support source. Applicants' specification, page 3, lines 1-5 and page 4, lines 18-21. The software trace may be conveyed, as a virus pseudo-signature, to the computer system. Applicants' specification, page 4, lines 18-21. Further, the component is a hardware device and the software trace is indicative of the presence of the hardware device in the computer system. Applicants' specification, page 5, lines 7-14.

Embodiments according to independent claim 15 describe an antivirus update system. The system comprises a reception element operative to receive software traces indicative of the presence, in a computer system, of a non-virus component. Applicants' specification, page 3, lines 8-13 and page 4, lines 18-23. The system further comprises a dispatch element operative to convey virus signatures to a plurality

of computer systems in addition to a pseudo-signature produced in response to the received software trace. Applicants' specification, page 3, lines 8-13 and pages 4-5, lines 29-1. The component is a hardware device and wherein the software trace is indicative of the presence of the device in the computer system. Applicants' specification, page 5, lines 7-14.

Embodiments according to independent claim 18 a method of detecting a non-virus component in a virus-protected computer system having antivirus software. The method comprises identifying a software trace indicative of the presence of a hardware device in the computer system, Applicants' specification, page 4, lines 13-15, and conveying the trace to the computer system as a virus pseudo-signature to allow detection of the device by the system's antivirus software. Applicants' specification, page 4, lines 18-21. The trace is conveyed to the computer system as part of an update procedure, whereby additional virus signatures or scanning engines may also be passed to the antivirus software. Applicants' specification, pages 4-5, lines 29-1.

Embodiments according to independent claim 21 describe a system of detecting a non-virus component in a virus-protected computer system having antivirus software. The system comprises means for identifying a software trace indicative of the presence of a hardware device in the computer system, Applicants' specification, page 4, lines 6-15, and means for conveying the trace to the computer system as a virus pseudo-signature to allow detection of the device by the system's antivirus software. Applicants' specification, page 4, lines 13-23. The trace is conveyed to the computer system as part of an update procedure, whereby additional virus signatures or scanning engines

may also be passed to the antivirus software. Applicants' specification, pages 4-5, lines 29-1.

#### **VI. Grounds of Rejection to be Reviewed on Appeal**

The following grounds of rejections are to be reviewed on appeal:

Claims 1-2, 4-10, and 12-21 have been rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Hypponen* (U.S. Patent No. 6,577,920) in view of *Kephart* (U.S. Patent No. 5,675,711).

Claim 11 has been rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Hypponen* in view of *Kephart* in further view of *Muttik* (U.S. Patent No. 6,963,978).

#### **VII. Arguments**

Claims 1-21 have been rejected under 35 U.S.C. § 103(a). Applicants respectfully traverse the rejection.

##### **A. The *Hypponen* Disclosure**

*Hypponen* describes an anti-virus software system that reports on a macro that is known to have a virus or is not known to the system and could therefore contain an unknown virus. *Hypponen* does not disclose identifying a software trace for a non-virus component, conveying the trace to a computer system to allow detection by the system's antivirus software, or does not disclose that such a component is a hardware device.

#### **B. The Kephart Disclosure**

*Kephart* describes a process of classifying a data string based on general features of the data string and not based upon a specific signature. See col. 1, lines 29-37 and col. 2, lines 49-54. *Kephart* also describes that data strings containing features of interest are used in addition with boot sectors that do not contain features of the class in order to train a program to recognize the features for a particular class of data. See col. 10, lines 19-39.

#### **C. The Muttik Disclosure**

*Muttik* describes a process for detecting viruses in software by comparing virus definitions with data that is under examination and by comparing the data with fingerprints of innocent data. Based on the results of these comparisons, security measures may be taken. See, e.g., col. 1, lines 57-67.

#### **D. Applicants' Claims 1-2, 4-10, 17, and 19-20**

As provided in independent claim 1, Applicants claim:

A method of detecting a non-virus component in a virus-protected computer system having antivirus software comprising:

*identifying a software trace of the non-virus component; and conveying the trace to the computer system as a virus pseudo-signature to allow detection of the non-virus component by the system's antivirus software,*

*wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the computer system.*

(Emphasis added).

Applicants respectfully submit that independent claim 1 is allowable for at least the reason that *Hypponen* in view of *Kephart* does not disclose, teach, or suggest at least "identifying a software trace of the non-virus component; and conveying the trace to the computer system as a virus pseudo-signature to allow detection of the non-virus component by the system's antivirus software, wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the computer system," as emphasized above.

*Hypponen* describes an anti-virus software system that reports on a macro that is known to have a virus or is not known to the system and could therefore contain an unknown virus. *Hypponen* does not disclose identifying a software trace for a non-virus component, conveying the trace to a computer system to allow detection by the system's antivirus software, or does not disclose that such a component is a hardware device. For at least these reasons, *Hypponen* does not disclose all of the features of claim 1.

With regard to *Kephart*, it describes a process of classifying a data string based on general features of the data string and not based upon a specific signature. See col. 1, lines 29-37 and col. 2, lines 49-54. *Kephart* also describes that data strings containing features of interest are used in addition with boot sectors that do not contain features of the class in order to train a program to recognize the features for a particular class of data. See col. 10, lines 19-39. As such, *Kephart* does not teach or suggest individually or in combination with *Hypponen* at least "identifying a software trace of the non-virus component; and conveying the trace to the computer system as a virus pseudo-signature to allow detection of the non-virus component by the system's

antivirus software, wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the computer system," as recited in claim 1.

As a result, claim 1 is patentable over *Hyponnen* in view of *Kephart*. Therefore, reversal of the rejection of claim 1 is respectfully requested.

Since claims 2, 4-10, 17, and 19-20 depend from claim 1 and recite additional features, claims 2, 4-10, 17, and 19-20 are allowable as a matter of law over the cited art of record.

#### **E. Applicants' Claim 11**

As provided in independent claim 11, Applicants claim:

A method of facilitating the detection of a non-virus component in a first virus-protected computer system comprising:

*identifying, on a second computer system, a software trace of the non-virus component, and conveying the trace towards an antivirus update source, whereby the software trace may be passed, as a virus pseudo-signature, to the first computer system, wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the first computer system.*

(Emphasis added).

Applicants respectfully submit that independent claim 11 is allowable for at least the reason that *Hyponnen* in view of *Kephart* in further view of *Muttik* does not disclose, teach, or suggest at least "identifying, on a second computer system, a software trace of the non-virus component, and conveying the trace towards an antivirus update source, whereby the software trace may be passed, as a virus pseudo-signature, to the first computer system, wherein the component is a hardware device and wherein the

software trace is indicative of the presence of the hardware device in the first computer system," as emphasized above.

*Hypponen* describes an anti-virus software system that reports on a macro that is known to have a virus or is not known to the system and could therefore contain an unknown virus. *Hypponen* does not disclose identifying a software trace for a non-virus component and conveying the trace to an antivirus update source, whereby the software trace may be passed, as a virus pseudo-signature, to the first computer system, wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the first computer system. For at least these reasons, *Hypponen* does not disclose all of the features of claim 11.

With regard to *Kephart*, it describes a process of classifying a data string based on general features of the data string and not based upon a specific signature. See col. 1, lines 29-37 and col. 2, lines 49-54. *Kephart* also describes that data strings containing features of interest are used in addition with boot sectors that do not contain features of the class in order to train a program to recognize the features for a particular class of data. See col. 10, lines 19-39. As such, *Kephart* does not teach or suggest individually or in combination with *Hypponen* at least "identifying, on a second computer system, a software trace of the non-virus component, and conveying the trace towards an antivirus update source, whereby the software trace may be passed, as a virus pseudo-signature, to the first computer system, wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the first computer system," as recited in claim 11.

With regard to *Muttik*, it describes a process for detecting viruses in software by comparing virus definitions with data that is under examination and by comparing the data with fingerprints of innocent data. Based on the results of these comparisons, security measures may be taken. As such, *Muttik* does not teach or suggest individually or in combination with *Hypponen* and *Kephart* at least “identifying, on a second computer system, a software trace of the non-virus component, and conveying the trace towards an antivirus update source, whereby the software trace may be passed, as a virus pseudo-signature, to the first computer system, wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the first computer system,” as recited in claim 11.

As a result, claim 11 is patentable over *Hypponen* in view of *Kephart* in further view of *Muttik*. Therefore, reversal of the rejection of claim 11 is respectfully requested.

#### F. Applicants' Claims 12-13

As provided in independent claim 12, Applicants claim:

A method of detecting, in a virus-protected computer system, the presence of a non-virus component comprising:  
*receiving a virus pseudo-signature associated with a software trace of the non-virus component, and*  
*comparing the pseudo-signature with software traces disposed within the system's memory,*  
*wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the computer system.*

(Emphasis added).

Applicants respectfully submit that independent claim 12 is allowable for at least the reason that *Hypponen* in view of *Kephart* does not disclose, teach, or suggest at

least "receiving a virus pseudo-signature associated with a software trace of the non-virus component, and comparing the pseudo-signature with software traces disposed within the system's memory, wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the computer system," as emphasized above.

*Hyponen* describes an anti-virus software system that reports on a macro that is known to have a virus or is not known to the system and could therefore contain an unknown virus. *Hyponen* does not disclose "receiving a virus pseudo-signature associated with a software trace of the non-virus component, and comparing the pseudo-signature with software traces disposed within the system's memory, wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the computer system," as recited in claim 12.

With regard to *Kephart*, it describes a process of classifying a data string based on general features of the data string and not based upon a specific signature. See col. 1, lines 29-37 and col. 2, lines 49-54. *Kephart* also describes that data strings containing features of interest are used in addition with boot sectors that do not contain features of the class in order to train a program to recognize the features for a particular class of data. See col. 10, lines 19-39. As such, *Kephart* does not teach or suggest individually or in combination with *Hyponen* at least "receiving a virus pseudo-signature associated with a software trace of the non-virus component, and comparing the pseudo-signature with software traces disposed within the system's memory, wherein the component is a hardware device and wherein the software trace is

indicative of the presence of the hardware device in the computer system," as recited in claim 12.

As a result, claim 12 is patentable over *Hypponen* in view of *Kephart*. Therefore, reversal of the rejection of claim 12 is respectfully requested.

Since claim 13 depends from claim 12 and recites additional features, claim 13 is allowable as a matter of law over the cited art of record.

#### **G. Applicants' Claim 14**

As provided in independent claim 14, Applicants claim:

Apparatus for detecting, in a virus-protected computer system, a non-virus component, comprising:

***a pseudo-signature generation element operative to produce a software trace of the non-virus component, and***

an antivirus support source,

***whereby the software trace may be conveyed, as a virus pseudo-signature, to the computer system,***

***wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the computer system.***

(Emphasis added).

Applicants respectfully submit that independent claim 14 is allowable for at least the reason that *Hypponen* in view of *Kephart* does not disclose, teach, or suggest at least "a pseudo-signature generation element operative to produce a software trace of the non-virus component . . . whereby the software trace may be conveyed, as a virus pseudo-signature, to the computer system, wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the computer system," as emphasized above.

*Hypponen* describes an anti-virus software system that reports on a macro that is known to have a virus or is not known to the system and could therefore contain an unknown virus. As such, *Hypponen* does not disclose at least “a pseudo-signature generation element operative to produce a software trace of the non-virus component . . . whereby the software trace may be conveyed, as a virus pseudo-signature, to the computer system, wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the computer system,” as recited in claim 14.

With regard to *Kephart*, it describes a process of classifying a data string based on general features of the data string and not based upon a specific signature. See col. 1, lines 29-37 and col. 2, lines 49-54. *Kephart* also describes that data strings containing features of interest are used in addition with boot sectors that do not contain features of the class in order to train a program to recognize the features for a particular class of data. See col. 10, lines 19-39. As such, *Kephart* does not teach or suggest individually or in combination with *Hypponen* at least “a pseudo-signature generation element operative to produce a software trace of the non-virus component . . . whereby the software trace may be conveyed, as a virus pseudo-signature, to the computer system, wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the computer system,” as recited in claim 14.

As a result, claim 14 is patentable over *Hypponen* in view of *Kephart*. Therefore, reversal of the rejection of claim 14 is respectfully requested.

## H. Applicants' Claim 15

As provided in independent claim 15, Applicants claim:

An antivirus update system comprising:  
*a reception element operative to receive software traces indicative of the presence, in a computer system, of a non-virus component, and*  
*a dispatch element operative to convey virus signatures to a plurality of computer systems in addition to a pseudo-signature produced in response to the received software trace,*  
*wherein the component is a hardware device and wherein the software trace is indicative of the presence of the device in the computer system.*

(Emphasis added).

Applicants respectfully submit that independent claim 15 is allowable for at least the reason that *Hypponen* in view of *Kephart* does not disclose, teach, or suggest at least "a reception element operative to receive software traces indicative of the presence, in a computer system, of a non-virus component, and a dispatch element operative to convey virus signatures to a plurality of computer systems in addition to a pseudo-signature produced in response to the received software trace, wherein the component is a hardware device and wherein the software trace is indicative of the presence of the device in the computer system," as recited and emphasized above.

*Hypponen* describes an anti-virus software system that reports on a macro that is known to have a virus or is not known to the system and could therefore contain an unknown virus. As such, *Hypponen* does not disclose at least "a reception element operative to receive software traces indicative of the presence, in a computer system, of a non-virus component, and a dispatch element operative to convey virus signatures to a plurality of computer systems in addition to a pseudo-signature produced in response to the received software trace, wherein the component is a hardware device and

wherein the software trace is indicative of the presence of the device in the computer system," as recited in claim 15.

With regard to *Kephart*, it describes a process of classifying a data string based on general features of the data string and not based upon a specific signature. See col. 1, lines 29-37 and col. 2, lines 49-54. *Kephart* also describes that data strings containing features of interest are used in addition with boot sectors that do not contain features of the class in order to train a program to recognize the features for a particular class of data. See col. 10, lines 19-39. As such, *Kephart* does not teach or suggest individually or in combination with *Hypponen* at least "a reception element operative to receive software traces indicative of the presence, in a computer system, of a non-virus component, and a dispatch element operative to convey virus signatures to a plurality of computer systems in addition to a pseudo-signature produced in response to the received software trace, wherein the component is a hardware device and wherein the software trace is indicative of the presence of the device in the computer system," as recited in claim 15.

As a result, claim 15 is patentable over *Hypponen* in view of *Kephart*. Therefore, reversal of the rejection of claim 15 is respectfully requested.

Since claim 16 depends from claim 15 and recites additional features, claim 16 is allowable as a matter of law over the cited art of record.

## I. Applicants' Claim 18

As provided in independent claim 18, Applicants claim:

A method of detecting a non-virus component in a virus-protected computer system having antivirus software comprising:

*identifying a software trace indicative of the presence of a hardware device in the computer system; and*

*conveying the trace to the computer system as a virus pseudo-signature to allow detection of the device by the system's antivirus software,*

*wherein the trace is conveyed to the computer system as part of an update procedure,*

*whereby additional virus signatures or scanning engines may also be passed to the antivirus software.*

(Emphasis added).

Applicants respectfully submit that independent claim 18 is allowable for at least the reason that *Hypponen* in view of *Kephart* does not disclose, teach, or suggest at least "identifying a software trace indicative of the presence of a hardware device in the computer system; and conveying the trace to the computer system as a virus pseudo-signature to allow detection of the device by the system's antivirus software, wherein the trace is conveyed to the computer system as part of an update procedure, whereby additional virus signatures or scanning engines may also be passed to the antivirus software," as emphasized above.

*Hypponen* describes an anti-virus software system that reports on a macro that is known to have a virus or is not known to the system and could therefore contain an unknown virus. As such, *Hypponen* does not disclose at least "identifying a software trace indicative of the presence of a hardware device in the computer system; and conveying the trace to the computer system as a virus pseudo-signature to allow detection of the device by the system's antivirus software, wherein the trace is conveyed

to the computer system as part of an update procedure, whereby additional virus signatures or scanning engines may also be passed to the antivirus software," as recited in claim 18.

With regard to *Kephart*, it describes a process of classifying a data string based on general features of the data string and not based upon a specific signature. See col. 1, lines 29-37 and col. 2, lines 49-54. *Kephart* also describes that data strings containing features of interest are used in addition with boot sectors that do not contain features of the class in order to train a program to recognize the features for a particular class of data. See col. 10, lines 19-39. As such, *Kephart* does not teach or suggest individually or in combination with *Hypponen* at least "identifying a software trace indicative of the presence of a hardware device in the computer system; and conveying the trace to the computer system as a virus pseudo-signature to allow detection of the device by the system's antivirus software, wherein the trace is conveyed to the computer system as part of an update procedure, whereby additional virus signatures or scanning engines may also be passed to the antivirus software," as recited in claim 18.

As a result, claim 18 is patentable over *Hypponen* in view of *Kephart*. Therefore, withdrawal of the rejection of claim 18 is respectfully requested.

#### J. Applicants' Claim 21

As provided in independent claim 21, Applicants claim:

A system of detecting a non-virus component in a virus-protected computer system having antivirus software comprising:

*means for identifying a software trace indicative of the presence of a hardware device in the computer system; and  
means for conveying the trace to the computer system as a virus pseudo-signature to allow detection of the device by the system's antivirus software,*

wherein the trace is conveyed to the computer system as part of an update procedure,

whereby additional virus signatures or scanning engines may also be passed to the antivirus software.

(Emphasis added).

Applicants respectfully submit that independent claim 21 is allowable for at least the reason that *Hypponen* in view of *Kephart* does not disclose, teach, or suggest at least "means for identifying a software trace indicative of the presence of a hardware device in the computer system; and means for conveying the trace to the computer system as a virus pseudo-signature to allow detection of the device by the system's antivirus software," as emphasized above.

*Hypponen* describes an anti-virus software system that reports on a macro that is known to have a virus or is not known to the system and could therefore contain an unknown virus. As such, *Hypponen* does not disclose at least "means for identifying a software trace indicative of the presence of a hardware device in the computer system; and means for conveying the trace to the computer system as a virus pseudo-signature to allow detection of the device by the system's antivirus software," as recited in claim 21.

With regard to *Kephart*, it describes a process of classifying a data string based on general features of the data string and not based upon a specific signature. See col. 1, lines 29-37 and col. 2, lines 49-54. *Kephart* describes that data strings containing features of interest are used in addition with boot sectors that do not contain features of the class in order to train a program to recognize the features for a particular class of data. See col. 10, lines 19-39. As such, *Kephart* does not teach or suggest individually or in combination with *Hypponen* at least "means for identifying a software trace indicative of the presence of a hardware device in the computer system; and means for conveying the trace to the computer system as a virus pseudo-signature to allow detection of the device by the system's antivirus software," as recited in claim 21.

As a result, claim 21 is patentable over *Hypponen* in view of *Kephart*. Therefore, reversal of the rejection of claim 21 is respectfully requested.

#### **VIII. Conclusion**

In summary, it is Applicants' position that Applicants' claims are patentable over the applied cited art references and that the rejection of these claims should be withdrawn. Appellant therefore respectfully requests that the Board of Appeals overturn the Examiner's rejection and allow Applicants' pending claims.

Respectfully submitted,

By:

  
Charles W. Griggers  
Registration No. 47,283

**Claims Appendix under 37 C.F.R. § 41.37(c)(1)(viii)**

The following are the claims that are involved in this Appeal.

1. A method of detecting a non-virus component in a virus-protected computer system having antivirus software comprising:
  - identifying a software trace of the non-virus component; and
  - conveying the trace to the computer system as a virus pseudo-signature to allow detection of the non-virus component by the system's antivirus software,
    - wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the computer system.
2. A method according to claim 1 wherein the trace is conveyed to the computer system as part of an update procedure, whereby additional virus signatures or scanning engines may also be passed to the antivirus software.
3. Canceled
4. A method according to claim 1 wherein the software trace is resident in a volatile area of the system's memory.
5. A method according to claim 1 wherein the pseudo-signature is tagged or otherwise marked to distinguish it from authentic virus signatures.

6. A method according to claim 5 wherein the antivirus software is modified so as to react differently to the presence of pseudo and authentic virus signatures.
7. A method according to claim 6 wherein the modification is effected as part of the update procedure.
8. A method according to claim 6 wherein the antivirus software does not attempt to fix, clean, modify or delete the component associated with the pseudo-signature.
9. A method according to claim 6 wherein detection of the pseudo-signature causes an advisory message to be conveyed to a user of the system, advising the user of the presence of the detected component.
10. A method according to claim 6 wherein detection of the pseudo-signature effects a connection to a website providing details of the component concerned.

11. A method of facilitating the detection of a non-virus component in a first virus-protected computer system comprising:

identifying, on a second computer system, a software trace of the non-virus component, and

conveying the trace towards an antivirus update source,

whereby the software trace may be passed, as a virus pseudo-signature, to the first computer system,

wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the first computer system.

12. A method of detecting, in a virus-protected computer system, the presence of a non-virus component comprising:

receiving a virus pseudo-signature associated with a software trace of the non-virus component, and

comparing the pseudo-signature with software traces disposed within the system's memory,

wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the computer system.

13. A method according to claim 12 wherein, in the event of a match being found, the antivirus software of the system is operative to convey, to a user of the system, an advisory message advising of the presence of the detected non-virus component.

14. Apparatus for detecting, in a virus-protected computer system, a non-virus component, comprising:

    a pseudo-signature generation element operative to produce a software trace of the non-virus component, and

    an antivirus support source,

    whereby the software trace may be conveyed, as a virus pseudo-signature, to the computer system,

    wherein the component is a hardware device and wherein the software trace is indicative of the presence of the hardware device in the computer system.

15. An antivirus update system comprising:

    a reception element operative to receive software traces indicative of the presence, in a computer system, of a non-virus component, and

    a dispatch element operative to convey virus signatures to a plurality of computer systems in addition to a pseudo-signature produced in response to the received software trace,

    wherein the component is a hardware device and wherein the software trace is indicative of the presence of the device in the computer system.

16. An antivirus update system of claim 15, wherein at least one of the plurality of computer system comprises an antivirus software element having a virus scanning engine and a signature table containing a plurality of virus signatures, the element also having a distinguishing capability whereby the element responds differently to the detection of virus signatures and virus pseudo-signatures, the latter being indicative of the presence of a non-virus component in the at least one computer system.

17. A method according to claim 1, wherein the antivirus software receives the virus pseudo-signature generated from the software trace of the component and scans the computer system so as to detect the presence of any component therein, having a matching software trace.

18. A method of detecting a non-virus component in a virus-protected computer system having antivirus software comprising:

identifying a software trace indicative of the presence of a hardware device in the computer system; and

conveying the trace to the computer system as a virus pseudo-signature to allow detection of the device by the system's antivirus software,

wherein the trace is conveyed to the computer system as part of an update procedure,

whereby additional virus signatures or scanning engines may also be passed to the antivirus software.

19. A method according to claim 1 wherein the pseudo-signature is tagged or otherwise marked to distinguish it from authentic virus signatures.

20. A method according to claim 19 wherein the antivirus software is modified so as to react differently to the presence of pseudo and authentic virus signatures.

21. A system of detecting a non-virus component in a virus-protected computer system having antivirus software comprising:

means for identifying a software trace indicative of the presence of a hardware device in the computer system; and

means for conveying the trace to the computer system as a virus pseudo-signature to allow detection of the device by the system's antivirus software,

wherein the trace is conveyed to the computer system as part of an update procedure,

whereby additional virus signatures or scanning engines may also be passed to the antivirus software.

**Evidence Appendix under 37 C.F.R. § 41.37(c)(1)(ix)**

There is no extrinsic evidence to be considered in this Appeal. Therefore, no evidence is presented in this Appendix.

**Related Proceedings Appendix under 37 C.F.R. § 41.37(c)(1)(x)**

There are no related proceedings to be considered in this Appeal.

Therefore, no such proceedings are identified in this Appendix.